David Engle

AMICON SYSTEM SPECIFICATION

Draft Revision 1.02
October 16th, 1981

This is a draft version of specifications for use of the data communications special service channels (L2) on the AMSAT Phase III satellites, the communications media which serve as the foundation of the AMSAT International Computer Network (AMICON). This document is subject to final approval by the Board of Directors of AMSAT. As a draft document it is subject to discussion, negotiation, further study, and potential rewrite of major sections. This document has not been approved for general publication. The contents herein represent the current thinking of the authors, and your comments and criticisms will be most welcome.

Comments and questions should be directed to:

AMICON System Architecture Design Group

c/o

H. S. Magnuski, KA6M, 311 Stanford Ave., Menlo Park, CA 94025
(415) 854-1927

FOREWORD

The Radio Amateur Satellite Corporation (AMSAT, P.O. BOX 27, WASHINGTON, D.C. 20044) will launch, courtesy of the European Space Agency, their Phase IIIB and Phase IIIC satellites sometime during 1982-1983. Unlike previous satellites OSCAR's 7, 8, etc., the Phase III machines will be in an orbit permitting extended communications periods for stations in the coverage area. Effective use of its 70 cm to 2 meter transponder will require more detailed planning and coordination than with previous OSCAR's, and a bandplan for the 180 kHz passband has already been approved by the AMSAT Board of Directors. Part of the plan makes provisions for six special service channels (General Voice Bulletins, Education Services, Scientific Services, Traffic, CW/RTTY bulletins and code practice, and Data Communications). The procedures for use of the Data Communications Special Service Channel, also known as Special Service Channel 'Lower 2' (SSC L2), is the concern of this document.

The explosive growth of the use of computers by radio amateurs, coupled with the potential of this new communications medium lead to fantastic possibilities for the establishment of two-way computer links, computer networks, packet radio gateways for long haul traffic, and even digitized voice or video. The realization of this potential, however, requires that communications standards be established so that common equipment and protocols can be used and shared by all interested operators. The standards must also consider and be compatible with other users of the spacecraft transponder. Thus, the contents of this document not only prescribe frequency assignments and modulation techniques, but also outline rules for time-shared use of the channel, packet layout, network protocols and other related matters.

The authors realize that standards are a two-edged sword, and have tried to obtain a balance between weak standards, which allow development in too many different directions, and overly restrictive standards, which could stifle creativity.

Contributors to this document include:

Vern Riportella	WA2LQQ	AMSAT Executive Vice President
H. S. Magnuski	KA6M	AMICON Coordinator
R.J. Carpenter	W3OTC	NBS Network Design Engineer

and many other radio amateurs who have offered constructive criticisms of the plans detailed herein.

PREFACE

Amicon System Specification for the AMSAT Phase III Satellite Channel L2

The AMSAT Board of Directors considering

a) that there is an urgent need for a common modulation method and accepted set of channel usage procedures (Level 1 Interface);

b) that there should be a specified format for transmitting message blocks over the channel (Level 2 Interface);

c) that there is a compelling need for coordination among the stations wishing to route messages and provide internetwork operations on the system (Level 3 Interface);

d) that future use of the channel would be greatly enhanced by commonly agreed to specifications for the end-to-end transfer of data (Level 4 Interface);

unanimously declares the view

that the following system specifications be adhered to by all stations using the special service channel for data communications on the AMSAT Phase III Satellites.

[Note: Text within square brackets in the following document is background discussion material designed to inform the reader of some of the issues involved in the design of the specification. It is not part of the formal document and is subject to deletion once the final draft is approved.

The current practice for specifying network architectures is to define independent functions in separate groups or layers. This document follows that design principle by proposing that AMICON follow the ISO model for Open Systems Interconnection. The first level deals with the transmission channel, the physical interface, and defines how a bit stream is transmitted between two stations. The second level superimposes characters and blocks of characters on the bit stream. This is called the link level. The third level describes how blocks of characters are routed through the network. The fourth level deals with the transmission of information which may span multiple blocks and which requires end-to-end checking. This is known as the transport level. In addition, there are three higher levels, not described here.]

Table of Contents

Chapter 1

LEVEL 1 INTERFACE: PHYSICAL INTERFACE

1.1 Channel Assignment and Characteristics

The AMSAT Phase III satellite has one inverting transponder with a 70 cm uplink and a 2 meter downlink. The bandplan assignment is based on the 2 meter downlink, which serves as the frame of reference. Subject to final calibration after launch, the passband center is 435.215 MHz for the uplink, and 145.900 for the downlink. There are two beacons marking the edges of the downlink passband, the lower "General" beacon at 145.810 MHz, and the upper "Engineering" beacon at 145.990 Mhz. The special service channels L1, L2 and L3 are allocated spectrum at 17, 21 and 25 kHz center frequencies above the General beacon. Channels H1, H2 and H3 are located at 17, 21 and 25 kHz center frequencies below the Engineering beacon. The L2 channel has been allocated for data communications and computer networking (nominally 435.284 MHz uplink, 145.831 MHz downlink).

The originating station must control the 70 cm uplink frequency such that the 2 meter downlink frequency (as monitored at the originating station) is at the specified offset from the pilot beacon to within a tolerance of +/- 1.0 kHz. Use of the SSCs with equipment incapable of this tolerance is discouraged.

[The 3 dB bandwidth being specified for the other channels is 2.4 kHz, and the data communications spectrum will probably have to meet this spec. The 1.0 kHz frequency tolerance was taken from the June 1979 AMSAT Newsletter, and may prove to be too loose for the L2 channel.] Looks like we might get ±5 kHz based on conference discussions.

1.2 Channel Access and Usage

In order to provide maximum channel utilization and to eliminate contention for channel time, a well organized system of coordinators and procedures is essential. Authority to use the channel comes from the AMSAT Phase III Operations committee. The special service channel coordinator member of the committee will appoint three regional coordinators to deal with channel usage in their respective regions. The regional L2 coordinator is responsible for assigning time slots for different modes of operation and L2 usage. Within a given timeslot, where the modulation and protocol implementations are compatible, access to the channel will be governed by the algorithms specified in Chapter 2.

1.3 Carrier and Modulation Specifications

[The selection of a suitable carrier and modulation scheme will be the subject of some debate within the amateur community, and currently there is no technique which can be considered the preferred method. The relative efficiencies of synchronous transmission probably will preclude any asynchronous modulation method. The following is a list of some of the considerations which are relevant to use of the L2 channel:

Power budget of the transponder
Channel 3db bandwidth or signalling speed in b/s per Hz.

Doppler shift
Frequency offset between sequential users of the channel
Eb/No (dB) for the modulation technique
Performance in the presence of cw interference
Channel capture capability
Complexity for the implementation
Cost of implementation and availability of hardware
Regulatory and licensing considerations

Some of the more frequently mentioned techniques are SSB, AFSK-FM, AQPSK-FM, and FSK. Karl Meinzer, in the June 1979 AMSAT bulletin, has outlined the use of uncoded PSK-SSB for the telemetry channel of the satellite. AFSK-FM is now in common use in the terrestrial packet local-area networks, and on the UOSAT telemetry channel. AQPSK-FM is possible with commonly found type 201 modems. Wide bandwidth FSK has been tried in an experimental way by some packet radio enthusiasts.

What we really need now is a written proposal covering the major modulation methods and an evaluation of each method in terms of the criteria outlined above. A summary of the principle methods includes:

AM - On-Off Keying with non-coherent detection
Quadrature Amplitude Modulation
Quadrature Partial Response

FM - FSK, non-coherent detection
CP-FSK, continuous phase FSK
MSK, minimum shift keying

PM - BPSK, binary phase shift keying
DE-PSK, differential encoded phase shift keying
QPSK, quaternary phase shift keying
OK-QPSK, offset keyed quternary phase shift keying

A very excellent and current summary of modulation methods for radio work can be found in 'A Comparison of Modulation Techniques for Digital Radio' by John D. Oetting, IEEE Transactions on Communications, Vol. COM-27 No. 12, December, 1979. This article would serve as a good basis for our comparisons of different schemes.]

1.4 Transmission Timing

The following description outlines a typical transmission. The times t0, t1, ... use as a point of reference the output antenna of the transmitting station. Note that there is a corresponding set of times s0, s1, ... which may be referenced at the output antenna of the transponder, and a third set r0, r1, ... which may be referenced at the receiver.

t0 - The transmitter places carrier on the channel. The transmitter assumes that the channel is idle and unused prior to t0.

t1 - Modulation is placed on the carrier such that all receivers assume a logical one or marking condition. Note that t1 may be the same as t0.

t2 - Denotes the start of the first idle flag or synchronization character.

t3 - Defines the transition between the last idling or synchronization character and the first byte of the packet.

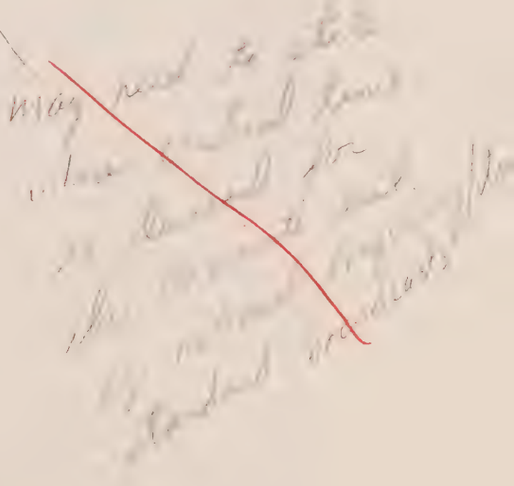
t4 - The time at the end of the last checksum or crc byte.

t5 - The time at the end of the last idle flag, sync character or pad character. The channel goes into a marking condition.

t6 - The instant that modulation is removed from the carrier. Note that t5 and t6 may coincide.

t7 - The removal of all carrier by the transmitter. This time may coincide with t6.

All stations must comply with the station identification requirements imposed by their licensing authority. However, since this channel may be heavily utilized, the time taken for id should be kept to the minimum allowed. All cw identification should occur between t0 and t3. [It has been suggested that an identification period, if it cannot be ruled out by an STA or rule change, be scheduled in the protocol for every ten minute period. This free-for-all ID time would meet the regulatory requirements.][A method for time synchronization is provided later in this paper]



Chapter 2

LEVEL 2 INTERFACE: PACKET TRANSMISSION SPECIFICATIONS

2.1 Packet Framing Specifications

The format of the message block or packet transmitted on the channel shall be in compliance with ISO Standard 3309 'High-level Data Link Control Procedures - Frame Structure.' Use of extended address and control fields, as detailed in the standard, is not recommended. The information field length within each packet shall be a multiple of 8 bits.

[The use of HDLC format could be controversial. The standards, techniques and equipment for the use of true, bit-oriented HDLC are still fairly new to the industrial world. The requirements for constructing an HDLC frame seem impossibly complex at first, and they would be except for the fact that many semiconductor companies have designed and are currently selling (for prices in the $30-$50 range) chips which do all the hard work. Here is a list of currently available HDLC oriented chips:

Fairchild 3846/6856	Synchronous Protocol Comm. Controller
Intel 8273, 8274	SDLC/HDLC Protocol Controller
Motorola 6854	Advanced Data Link Controller
Motorola 68561	Multi-protocol Controller
Nippon Electric Co. UPD379	SDLC Protocol Controller
Nippon Electric Co. UPD7201	SDLC Protocol Controller
Signetics 2652	Multi-protocol Controller
Standard Microsystems 5025	Multi-protocol Controller
Western Digital 1933	Synchronous Data Link Controller
Zilog SIO	Serial I/O Controller

The HDLC protocol is being designed into new equipment by all major manufacturers, and it forms the basis for the new international packet switching networks. It will be the standard for data communications in the eighties. If we are in the process of creating a digital networking specification for use over the next ten years, we should build on what is currently accepted industrial practice, even though most amateurs may be unfamiliar with the details involved. Several groups of Canadian and U.S. operators have already conducted experiments using HDLC chips and established networks based on HDLC, so we have evidence that the technology is not out of reach of the amateur community. Several other groups in the U.S. have also adopted HDLC as their standard. The main drawback with specifying bit-oriented HDLC is that it is incompatible with commonly used USARTs, such as the 8251A.

Also, note that this spec only calls for frames from the HDLC standard. The complete HDLC protocol is probably not appropriate for our multiple-access broadcast oriented packet repeater.

A question has been raised as to the legality of use of HDLC frames in the U.S. and other countries. In opening up radio communications to ASCII, the FCC only specified Baud rates, and did not rule on formats for start/stop bits, synchronous protocols, etc. The U.S. version of HDLC is an ANSI Standard, X3.66-1979, Advanced Data Communication Control Procedure. We need a legal

opinion on use of this standard by U.S. amateurs. If HDLC framing is also outlawed in many other countries, or if waivers cannot be easily obtained, then it would be unwise to spec it for the satellite.]

2.2 Transmission Code

The transmission code used for text characters within the message shall meet the standards set by C.C.I.T.T. Recommendation V.3 - International Alphabet No. 5.

[This is the international standard corresponding to ANSI Standard X3.4-1968 'Code for Information Interchange - ASCII.']

Bit insertion and removal, as required by the HDLC specifications, is assumed.

2.3 Channel Multiple Access Protocol

When channel usage is low, packets may be transmitted using pure-ALOHA protocol. When utilization becomes heavy, packets will be exchanged on the channel using an S-ALOHA protocol with closed loop control.

2.3.1 Definitions

A multiple-access-channel is a communications channel where many transmitting stations can attempt to access a receiving station using a common transmission medium and equipment. The uplink to the Phase-III satellite is a multiple-access channel.

A broadcast-channel is a communications channel where many stations can receive messages from a single transmitting station. The downlink of the Phase-III satellite is a broadcast channel.

The term carrier-sensed multiple-access channel (CSMA) describes a situation where each transmitter is able to detect the carrier (presence of an on-going transmission) from all other transmitters. The Phase III input channel has this characteristic except for the fraction of a second delay at the beginning of a transmission when the input signal has to travel to the satellite and return to receiving groundstations. The use of carrier sensing improves channel efficiency, particularly for longer packets.

The term 1-Persistent CSMA describes a situation where a station transmits a packet immediately if the channel is sensed idle, and if not found idle, waits until the channels goes idle and then transmits immediately. The term Non-Persistent CSMA describes a situation where a station transmits a packet immediately if the channel is sensed idle, and if sensed busy, reschedules the transmission for some later time according to the rules for retransmission delay distribution. The term p-Persistent CSMA describes a situation where a station waits for the channel to go idle, and then delays the start of transmission for a prescribed period, the exact delay depending on the retransmission delay distribution and on other activity on the channel.

Due to the fact that transmissions are occuring at random with no centralized control, there is the possibility of overlap of transmitted packets or collisions, where two or more transmitters are on the air at the same time. For efficient use of the channel it is important that each station be able to

monitor its translated signal and check the validity of the returned packet while it is being transmitted. This ability to receive one's own packets and validate their contents is called a collision detection capability.

At any given time, using the output antenna of the transponder as our point of reference, the channel will be either be inactive with no carrier present or active with carrier. The channel duty cycle is the percentage of time that the channel is active. This measurement should be made over an extended period of time, at least 15 minutes or more.

A set of rules and procedures for controlling the exchange of messages on a communications channel is a communications protocol. Of the many hundreds of communications protocols currently in use there is a set of protocols, known as ALOHA protocols, which are concerned with regulating the flow of messages or packets on communications media where the messages are sent using a multiple-access channel and received on a broadcast channel. The name 'ALOHA' is used because much of the initial research and the first implementations were done by the University of Hawaii in the construction of their ALOHA Packet Radio Network.

A pure-ALOHA protocol allows any station on the network to transmit whenever it's ready. If the transmitted packet is not received correctly, the transmitter waits some random amount of time and tries again.

A slotted-ALOHA protocol (S-ALOHA) requires that all transmissions on the multiple-access channel be synchronized to start and end within specified time periods or slots. All slots are of the same duration and can contain the maximum length packet. Each transmitter decides on which time slot to use on a random basis.

A slotted-ALOHA closed-loop-control protocol (S-ALOHA-CLC) allows transmitting stations to adjust their transmission control parameters to accomodate varying load conditions on the channel. Each transmitted packet contains a computed variable which reflects, in part, the success that the transmitting station is having in sending packets. All receiving stations monitor this variable and adjust, through use of the algorithms and formulas specified below, their transmit and retransmit controls. Closed loop control of an ALOHA channel allows throughput to approach theoretically maximum limits, provides a mechanism for dynamic changes in the control parameters needed to cope with varying loads, minimizes overall packet delay, and contributes to the efficient use of the channel under heavy load conditions.

2.3.2 Control Parameter Notation

The notation and control algorithms given below were adapted from a paper written by Gerla and Kleinrock (see the bibliography, Appendix A). Their careful study and contribution to the solution of this control problem is acknowledged.

Specification of the ALOHA control procedures uses the following variables:

n - The number of stations currently actively using the L2 channel.

i - Stations are indexed by the variable 'i' where i ranges from 1 to n.

tau - The time in seconds required to transmit a maximum length packet.

ts - The period of a slot in a slotted channel.

W - The history window (measured in slots) maintained by each station.

E - The number of empty slots in W.

S(i) - Successful packets from station i in W.

S - Total successes in W. Computed by summing all S(i) for i = 1 to n.

C - The total number of collision slots in W.

$$C = W - (S + E)$$

C(i) - Collisions suffered by station i in W.

C'(i) - A station's estimate of the total number of collisions in W.

$$C'(i) = (C(i)/S(i))*S$$

m - Average number of collided packets per collision. Note that this parameter cannot be measured directly through monitoring the channel.

UC - Interval (in slots) between successive updates of control parameters. Note that UC will be less than or equal to W.

G - Average channel load in window. Computed through the formula:

$$G = (S+C*m)/W$$

In the closed loop control algorithm presented below G will only be estimated because the true value of m is not available.

Gmax - A ceiling value for the G estimate.

Pn(i) - New transmission probability gate value for station i. At each transmission decision point (the time when a new packet is ready for transmission in the pure-ALOHA protocol or the time when a new packet is ready and we have the start of a slot for the slotted-ALOHA protocol) the transmitter draws a random number ranging from zero to one. If the number picked is less than or equal to Pn(i), then transmission commences. For the pure protocol Pn(i) = 1 and transmission always occurs immediately, providing the channel is inactive (there is no carrier at the transmit site). The initial value of Pn(i) is Pn. [A method for determining Pn(i) is provided later in this paper]

Pr(i) - Retransmit probability gate value for station i. At each transmission decision point Pr(i) is used to determine if a previously transmitted packet should be retransmitted. Packets will need retransmission if they are not positively acknowledged by the receiver or if the transmitter detects an error or collision through its own monitoring of its transponded output. All packets that need retransmission must be sent first before any new packets are attempted (the retransmit packet queue has a strictly higher priority than the new packet queue). In the pure-ALOHA protocol the

retransmit all packets from th... determined in error packet, Don't depend on receiver keeping out of sequence packets fill in the gaps

transmission decision points occur every tau seconds after an error is detected. In the S-ALOHA protocol there is a decision point at the beginning of each slot. The initial value of Pr(i) is Pr. [a method for determining Pr(i) is provided later in this paper.]

Prmax - Ceiling value for Pr(i).

P - The weighted average of all current gate values. The value P is computed by summing Pn(i)*S(i) for all i and dividing by S. The value of Pn(i) is contained in a control byte in each transmitted packet. S(i) is obtained by monitoring the channel and is based on successfully received packets.

DP - The gate value increment. This parameter is used to compute the new values of Pn(i) and Pr(i) and controls their rate of change.

2.3.3 Control Using ~~the Pure-ALOHA~~ Algorithm

If the channel duty cycle is less than 25% there is no justification for requiring closed loop control and simple control procedures will suffice. The pure-ALOHA channel throughput reaches a theoretical maximum of 18% when the channel duty cycle reaches 50%. The protocol, in its most basic form, follows these two steps:

1. When a station has a new packet ready to transmit, it transmits it.

2. If the packet was not received correctly, the station waits some random amount of time and then retransmits the packet.

The following paragraphs will clarify some of the details concerning the above two steps.

2.3.3.1 ~~Pure-ALOHA~~ Transmission Control

First, in this section and the next we differentiate between new packets and ones that have been previously transmitted. The probability of transmission control gates Pn(i) for new packets and Pr(i) for retransmitted packets have different values. Pn(i) for this protocol is always 1, implying that transmission will be immediate. Pr(i) will be assigned a value when the network starts up, and may be subject to change as the load grows. The priority of packets due for retransmission is strictly higher than that of new packets. We will also restrict each station to have only one unconfirmed packet in the air at any given time. Due to the round-trip signal delays involved, in theory it is not absolutely essential that stations hold back transmissions if there is already carrier present on the output channel. The carrier may already be off at the transmitter site using the channel. Carrier sensing will, however, improve throughput, so it is recommended that new transmissions not start if the channel is already active.

[The inclusion of carrier sensing converts the protocol from Pure-ALOHA to a CSMA protocol. The scheme given here is more properly called 1-persistent CSMA. Sherman, et al., Data Communications, July 1978, show that 1-persistent CSMA equals slotted-ALOHA (maximum throughput 36% of bit rate) when the propogation delay is one-fourth of the packet duration; these are the conditions to be expected in Phase III. CSMA is poorer than slotted-ALOHA for a larger delay/packet duration ratio, becoming worse than Pure-ALOHA when the delay is 8/10 of the packet duration. Also, the limitation of the acknowledgement window

size to one will result in a lot of small ACK packets, which will waste system throughput. Do we need to do ACKs at the Link Level, and if so how?]

2.3.3.2 Pure-ALOHA Retransmission Control

Packet reception may be confirmed in two different ways. The term 'end-to-end' confirmation is used when the higher level processes or programs doing the packet transmitting and receiving positively acknowledge the reception of a new packet. The other confirmation of successful transmission comes from the transmitter's own receiver and its collision detection circuits. Collision detection circuitry does not guarantee safe reception at the final or ultimate receiver, but it does permit the transmitter to immediately reschedule a packet if it is known to be in error, thus avoiding positive acknowledgement timing delays.

The exact procedure for 'waiting a random amount of time' will now be described. This procedure is used for the pure-ALOHA protocol because it is consistent with the closed-loop method which follows below.

A station which has determined that it needs to retransmit first waits for the channel to go inactive. It then picks a random number in the range 0 to 1, and if this number is less than or equal to Pr(i) it retransmits immediately. If the number is greater than Pr(i), it delays tau seconds, picks a new random number and repeats the test. This cycle is continued until the retransmission occurs.

By using some mathematical tricks we can simplify the above series of tests and still achieve the same result. Again, we wait for the channel to go inactive and then pick a number in the range 0 to 1. The time we should wait, twait, is then given by the following formula:

$$twait = random.number * tau * (1-Pr(i))/Pr(i)$$

The value of twait may be rounded to the nearest tau seconds. If the channel is busy when the time delay expires, the station should wait for the channel to go inactive and then transmit immediately.

[The proposal for retransmission is really p-Persistent CSMA. It, too, doesn't help much with packets that are not much longer than the propagation delay. Should we use a different protocol for retransmissions than for the first transmission? The extra complexity may not be necessary.]

2.3.3.3 Pure-ALOHA Control Parameter Values

There are only two parameters subject to adjustment in the Pure-ALOHA control algorithm. Consult AMSAT for currently recommended values of control parameters. Typical values for these parameters are listed below:

tau = 1 second
Pr(i) = Pr = .4

2.3.4 Control Using the S-ALOHA-CLC Algorithm

If the channel duty cycle becomes greater than 20%, then there is enough activity on the channel to justify control procedures which will guarantee

better throughput under heavy loading and under varying load conditions. The Slotted ALOHA Closed Loop Control algorithm is a method whereby the transmit and retransmit probabilities Pn(i) and Pr(i) are adjusted to accomodate the current channel load, the adjustment causing stations to wait longer when many transmitters are competing for the channel, and then shortening the delay times as traffic is cleared and channel conditions improve.

The key elements of the CLC method are these:

All transmitters are synchronized and start and end their transmissions within fixed time slots. Each transmitter monitors the total number of successfully received packets within a recent time period (the 'history window', measured in time slots), and also keeps a count of its own successes and failures within the window. Each packet transmitted by station i contains a control byte which reflects the current value of Pn(i) for that packet. The Pn(i) values in each packet are recorded by all active stations and their values are used in load calculations specified below. With the data thus recorded, a formula is used to update, at predetermined intervals, the Pn(i) and Pr(i) for the station. Increasing values of Pn(i) or Pr(i) imply that every station in the net is having more success and that less delay is required before transmit and retransmit attempts. As the values of Pn(i) and Pr(i) decrease more delay is introduced causing all stations to slow down, thus reducing channel congestion. The following sections give the exact details of the method.

2.3.4.1 Closed Loop Control Assumptions

This method assumes that channel time is divided into fixed periods or slots, where each slot is ts seconds long and can contain the maximum length packet plus transmitter startup and shutdown time. All slots will start and end on the second's tick from WWV.

[Stations can easily compute the ionospheric propagation delay between themselves and WWV, and should be able to get within 20 milliseconds or so of true synchronization. Likewise, the delay difference to the satellite from a station at the subsatellite point and one on the limb of the Earth should be less than ten milliseconds - for a total synchronizing error of less than about 30 milliseconds as seen by the satellite. This seems very acceptable with one-second slots.]

Each active station keeps certain statistics over the last W slots and updates its control parameters every UC slots. The update period, UC, will be less than or equal to W.

The station must monitor the channel and count all successfully received packets S. It must also count its own successes S(i).

Finally, at each update interval the station must compute the weighted average of current gate values. The current Pn(i) value for each station is transmitted in the packet in the protocol load control byte which is the byte immediately following the HDLC control field. The right-hand 7 bits of this byte divided by 128 represent Pn(i) for that packet. Use of the high order bit is reserved and it should be set to zero. Stations which are not using closed loop control will set this byte to hex '00'. The weighted average gate value, P, is the sum of all received Pn(i) divided by S.

2.3.4.2 Closed Loop Control Algorithm

The following formulas must be used by each station to update Pn(i) and Pr(i) every UC slots.

(a) Estimate Collisions:

If C(i) = S(i) = 0 then:

If S = 0, let G = 0 and go to (c)
Otherwise, let G = 1 and go to (c)

If C(i) > 0 and S(i) = 0 then:

Let G = Gmax, P = min(P,Pn(i)) and go to (c)

If S(i) > 0 then:

Let C'(i) = C(i) * S / S(i) and go to (b)

(b) Estimate total channel load G:

$$G = (S + C'(i))/W \quad \text{with} \quad 0 \leq G \leq Gmax$$

(c) Derive new probability gates:

$$Pn(i) = P - (G - 1) * DP \qquad 0 \leq Pn(i) \leq 1$$

$$Pr(i) = \min(Pn(i), Prmax) \qquad 0 \leq Pr(i) \leq 1$$

2.3.4.3 Slotted ALOHA CLC Parameter Values

Consult AMSAT for currently recommended values of control parameters. The following are typical values:

ts = 1	Slot size in seconds
W = 64	History window (slots)
UC = 16	Update period (slots)
Pn = .5	Initial new packet transmit gate
Pr = .1	Initial retransmit packet gate
Prmax = .5	Ceiling value for Pr(i)
DP = .25	Probability increment
Gmax = 2	Ceiling value for G estimate

[Some simulation studies are required to properly analyze the effect of changes in the control parameters and to determine which features of the protocol are really useful and which can be discarded. Here is a list of some questions which need investigation:

1. Performance curves for Pure-ALOHA
   a. Effect of changing packet length.
   b. Effect of carrier sensing.
   c. Variations caused by changing Pr(i).

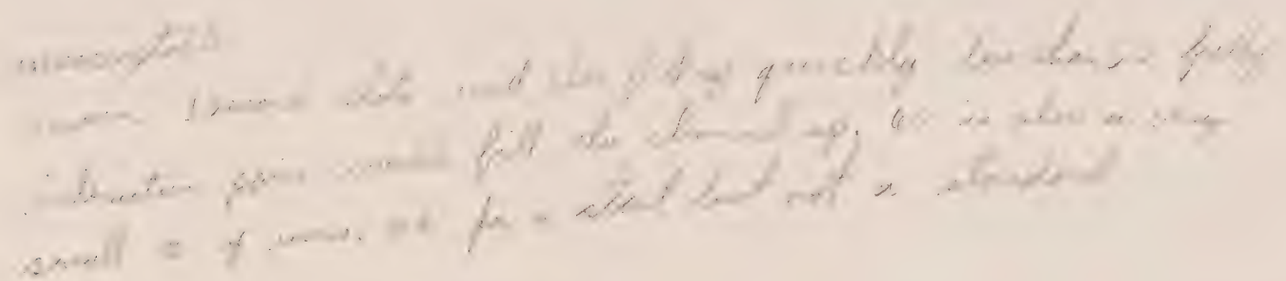
2. Performance curves for S-ALOHA-CLC

a. Effect of changing packet length.
b. Effect of carrier sensing.
c. Benefits of slotting.
d. Parameter settings and optimal values.

3. Determining the optimal load level to switch from the Pure-ALOHA to S-ALOHA-CLC.

The simulation could be written in PASCAL using discrete time steps.

Perhaps we should give more attention to some of the protocols mentioned by Lam (IEEE Transactions on Communications, October 1979). In particular, he describes a protocol in which time on the satellite is divided into a fixed sequence of N slots, repeating regularly. A station uses CSMA protocol to capture one train of these slots. This is a trick which effectively makes the packet durations much longer (and interleaves them) so that the long Earth-Satellite-Earth delays don't wreak as much havoc. Since the specification has shown how easy it should be for hams to synchronize their time bases, this approach looks attractive. It does strictly limit the number of active pairs or groups of stations to N, at any instant; however the datagram (or X.25 Quick Select) approach could spread this across many more stations. Obviously N would have to be widely published and strictly adhered to. Probably a value of N = 4 to 8 would be all that could be tolerated. Each train of slots only returns 1/N times the channel bit rate (though all N trains give this value simultaneously).]



Chapter 3

LEVEL 3 INTERFACE: NETWORK SPECIFICATIONS

3.1 Datagram Network Characteristics

The architecture of data communications networks in use today is diverse and many different types of connecting arrangements are possible. There are point-to-point connections, multi-point networks, switched circuits, virtual circuits, switched virtual circuits, etc. The AMICON network is one example of a fully-connected packet switching network. The term fully-connected is used because there is the possibilty of a connection from every station in the net to every other station (through use of the multiple-access broadcast channel). The network is a packet switching network because all user information is broken into small packets of data, allowing many different users to have multiplexed access the channel.

The technology of building packet switching networks is under active development currently, and there are many different types of packet switching services available today. The type of service that best characterizes the AMICON network is referred to as a datagram service:

A datagram is a self-contained packet which carries sufficient information such that it can be routed from source station to destination station without reliance on any previous exchanges between source and destination and the communications network. The data field within a datagram will be kept intact and not split-up or altered in any way by the network.

The delivery of a datagram is not guaranteed. There is a high probability of delivery, but it may occasionaly be lost. The data within a properly received datagram, however, will have an extremely low probability of error.

The sequence in which datagrams are supplied by sender is not necessarily the sequence in which they will be received by the receiver. All datagrams in transit in the network are treated as independent entities.

Under some circumstances it is possible for a duplicate transmission to occur, causing the same datagram to appear more than once at the receiver.

In summary, a datagram service is an extremely simple but fairly fast transport service which serves as the foundation on which higher level communications protocols are built. These higher level protocols (Level 4 and above) are responsible for end-to-end acknowledgments, sequence checking, retransmissions of lost packets, flow control and other controls which will guarantee a complete and orderly passage of data from sender to receiver.

3.2 Packet Format

The packets or datagrams flowing through the AMICON network will have the format described below:

Bytes	Field	Description
1 to n	Framing	Initial framing or synchronization bytes
1	Address	HDLC address byte
1	Control	HDLC control byte
1	Protocol	Protocol load-control byte
20 to n	Header	Network Level Protocol Header
0 to n	Data	Datagram data field (unrestricted in content)
2	CRC	Packet checksum bytes
1 to n	Framing	Terminating framing or pad characters

The initial framing or synchronization bytes are not detailed here. The beginning-of-packet control sequence is described in the Level 2 description of a packet.

The HDLC address field consists of a single byte. Use of extended address fields, as provided for in the standard, is not recommended. The contents of this address field are not used by the Level 3 protocol. Packets which are used for testing should set the address byte to hex '00'. Packets which are not using the address byte for higher level protocol functions should set this byte to the all-parties-addressed code, hex 'FF'. The contents of this byte, if used, must conform to any specifications given in Chapter 2 on the Link Level Interface.

[Not using the address field (at the Link Level) wastes the address recognition feature of the HDLC chips, and imposes considerable overhead on the higher level by servicing of packets intended for other stations. Normally the Link Level address(es) would be of the two parties to a link level exchange. The Link Level addresses just point to way-points on the path between the end-to-end addressees.]

The HDLC control field consists of one byte. Use of an extended control field, as provided for in the standard, is not recommended. The contents of the control field are not used by the Level 3 protocol. Stations not using this byte for control purposes should set it to hex '03', which is an HDLC Unnumbered Information frame. The contents of this byte, if used, must conform to any specifications given in Chapter 2 on the Link Level Interface.

The protocol load-control byte is used by the S-ALOHA-CLC protocol control software. The contents of this byte are detailed in the Level 2 description of the closed-loop-control algorithm. Stations not using closed loop control should set this byte to hex '00'.

The packet network-header field is described in Section 3.3 below.

The packet data field is described in Section 3.4 below.

The two cyclic-redundancy-check (CRC) bytes provide error checking for the contents of the packet. The contents of these bytes are detailed in the Level 2 description of the packet.

The terminating framing or pad bytes are described in the Level 2 description of the packet.

3.3 Packet Network-Level Protocol Header

The packet network-level protocol header must contain the following key items of information:

1. 'From' and 'To' callsigns.
2. 'From' and 'To' local area network addresses.
3. A unique identifier code.
4. Time-to-live or hop-count field.
5. Protocol-type code.

In addition some other auxilliary information may be included, such as fragment control fields, type of service options, routing directives, packet lengths and checksums, and variable options fields.

The DOD Standard INTERNET Protocol network header meets these requirements and is recommended for adoption intact. Appendix C contains partial specifications for the INTERNET protocol. The source document is available from the NTIS, document number ADA 079 730. The specification was also reprinted in the ACM Computer Communication Review, October 1980, Volume 10 Number 4, pages 12 - 51.

Two modifications to this header are required to fulfill the requirements for amateur packet radio service:

The first consideration concerns the 32-bit fields used for source-address and destination-address. The first byte of this four byte field represents a network, and Network Number 44 (decimal, conveniently half of that famous number 88) has been assigned to the Amateur Packet Radio Network. That leaves three bytes or 24 bits of addressing, a selection of 16,777,216 integers which can be assigned to unique entities in our network. That number is large enough to assign each amateur on earth a unique code. Doing that, unfortunately, does not help the routing problem very much because one would need a callbook type of directory to translate these digits into people or places. It also does not take advantage of the uniqueness of callsigns and our familiarity with and use of calls. We propose to utilize the 24 bit address field in the following manner:

> Addresses only have to be assigned to stations serving as network traffic processors, such as repeaters, gateways and mailboxes, and other individual stations do not have to have an address if they are accessible via a local net served by such a gateway or repeater.
>
> The high order 16 bits (65,536 integers) can be assigned to stations based on their geographic location. It turns out that 360 degrees longitude multiplied by 180 degrees latitude provides for 64,800 locations, just under the 65,536 permitted. The remaining low order 8 bits can be sequentially assigned to stations within the same

geographic area. If all 256 slots are filled, the nearest open slot can be assigned. Numbers above 64,800 are reserved for satellite stations and special cases. This method of address assignment is both rational and allows repeaters to implement message routing without any prior knowledge of the location of the recipient.

The callsigns of the sender and receiver will be located in the options field, using two of the unassigned control option numbers. Thus the packet header will consist of the standard 20 bytes plus 12 to 16 bytes of options containing the sending and receiving callsign. Explicit routing of messages is still permitted through use of the source routing option.

Some of the complexity of the INTERNET standard could be reduced by restricting use of the following features:

Fragmentation - Breaking up a packet is not necessary if the buffer allocation is large enough. The standard specifies a 576 byte maximum packet size.

Service Type - This is an option which can be ignored. Useful for interactive vs. batch traffic, or priority message handling.

Security Option - Not required in our network.

Stream Id - Not required

Timestamps - Optional

When we eliminate the requirement for the above items, we really have a basic set of features which are needed for an easy-to-use and versatile network service. Some of the features, such as error reporting, will be necessary to help people figure out what's going on. Other optional features will be useful in testing and measuring network performance.

[This protocol is a standard, adopted by the DOD, ARPANET, and supported by many other major packet carriers. It represents the experience of ten or more years of computer networking and the contributions of hundreds of researchers and developers of packet technology. The specification is complete, a publicly available document (through NTIS), and can be used in a fairly simple way by our network. It provides us with the datagram building basis which I feel is important. It conforms to currently accepted practices of multi-layer network design, and could be used both on a national and international basis.

It would make us compatible with DoD and some other networks to which we might eventually want to interface. Amateurs have had a long history of cooperation with the military (MARS, for example) and this would represent a continuation of that cooperation.

It would save us an enormous amount of development time in bringing up our network. I'm really afraid that if we started with something much simpler, as some hams will encourage us to do, we would find in a year or two that features are lacking and extensions are necessary. Much discussion and haggling would produce a new and revised spec, and piece by piece we would eventually reinvent most of the features that are currently in the INTERNET document. I think it's

much more reasonable to take this design and declare certain features as optional for our network.

Counterproposals to the adoption of INTERNET Protocol are most welcome.

We think that the protocol would work for us, and serve our needs in a reasonably economical manner. The INTERNET protocol permits us to adopt TCP or some other set of end-to-end protocols in the next higher layer of the network. It allows us to use HDLC as the link level and local area network mechanisms for delivering packets to the end-user stations. It's compatible with what we need for the satellite net. It has some really neat features, and we would like to see some comments on why we shouldn't use it.]

3.4 Packet Data Field

The datagram packet data field contains data or control information which the sender desires to transmit to the receiver. The contents of this field are not interpreted by Level 3 software. The only constraint is that the length of the data field plus the control and addressing fields must not exceed the maximum packet length.

Chapter 4

LEVEL 4 INTERFACE: TRANSPORT LEVEL PROTOCOL

4.1 Transport Level Protocol

The protocol required for the end-to-end transmission of information through the network will not be covered by this revision of the specification and is a subject for further study.

[ARPANET uses a file transfer protocol known as TCP. It would be a good starting point and perhaps we can adopt a compatible subset for our use. The original reference material for TCP may be found in 'A Protocol for Packet Network Intercommunication' by Vinton G. Cerf and Robert E. Kahn, IEEE Transactions on Communications, Vol. COM-22, pp. 637-648, May, 1974.

The DOD has adopted a version of TCP for their networks. This document is available through the NTIS as publication number ADA 082609. It has also been published in the ACM Computer Communication Review, October 1980, Volume 10 Number 4, page 52.

We have not recommended the adoption of TCP because it may be too cumbersome for our needs, an overkill, and may require too much in the way of machine resources.]

Chapter 5

SESSION CONTROL, PRESENTATION AND APPLICATIONS PROTOCOLS

5.1 Session Control Protocol

The protocol required for session connection on the network will not be covered by this revision of the specification and is a subject for further study.

5.2 Presentation Protocol

The protocol required for presentation services will not be covered by this revision of the specification and is a subject for further study.

5.3 Application Protocols

The protocol required for specialized applications such as digitized voice or video will not be covered by AMICON specifications.

Appendix A - Selected Bibliography

REFERENCES ON PERSONAL COMPUTER NETWORKS

The Making of an Amateur Packet Radio Network
Borden, David W., and Rinaldo, Paul L.
QST, Vol. LXV Number 10, October 1981. p. 28-30.

AMRAD Newsletter "Protocol" Column
Borden, Dave, Route 2, Box 233B, Sterling VA, 22170

A Multiuser Data Network - Communicating over VHF Radio
Bruninga, Robert E., 907 Ninovan Road, Vienna, VA 22180
BYTE, Vol. 3 No. 11, p. 120, November, 1978

Design Considerations For A Hobbyist Computer Network
Caulkins, D., 437 Mundel, Los Altos, CA 94022
Proceedings of the First West Coast Computer Faire, April, 1977

PCNET 1979
Caulkins, D., 437 Mundel, Los Altos, CA 94022
People's Computers, Vol. 6 No. 2, Sep-Oct 1977

Dial-up Directory
Derfler
73 Magazine, January 1980 and after

Hobbyist Computerized Bulletin Board
Christensen, Ward, 688 E. 154th St. #3D, Dolton, IL 60419
Suess, Randy, 1930 Bradley, Chicago, IL 60613
BYTE, Vol. 3 No. 11, p. 150, November, 1978

Community Memory - A 'Soft' Computer System
Felsenstein, L.
Proceedings of the First West Coast Computer Faire, April, 1977

Homebrewery vs. The Software Priesthood
Fylstra, d.
Wilber, M.
Byte, October, 1976

Hip Packet
Halprin
QST, April 1981, p. 91.

ASCII, Baudot and the Radio Amateur
Henry
QST, September 1980, p. 11.

An Introduction to Packet Radio
Hodgson
HAM RADIO, June 1970, p. 64

Distributed Network
Horton, Glen, Hickock Teaching Systems, 2 Wheeling Ave., Woburn, MA 01801
BYTE, Vol. 3 No. 11, p. 62, November, 1978

Standards for Personal Computing Networks
Isaak, Jim
IEEE Computer, October, 1978 p. 60

The Sky's the Limit: Ham Radio for Intercomputer Communication
Kassar, Joe, 11532 Stewart Lane, Silver Spring, MD 20904
BYTE, Vol. 3 No. 11, p. 48, November, 1978

The Club Computer Network
Kassar, Joe, 11532 Stewart Lane, Silver Spring, MD 20904
BYTE, Vol. 5 No. 5, p. 202, May, 1980

Interpersonalized Media: What's News?
Levin, James A., University of California, San Diego, La Jolla CA 92093
BYTE, Vol. 5 No. 6, p. 214, June 1980

DIALNET And Home Computers
McCarthy, J.
Earnest, L.
Proceedings of the First West Coast Computer Faire, April, 1977

Why not Just Use the Phone?
Newcomb, Donald R., 819 Bayou Blvd., Pensacola, FL 32503
BYTE, Vol. 3 No. 7, p. 121, July, 1978

Washington Mailbox: ASCII
Palm
QST, June, 1980, p. 60

CB Computer Mail
Pank, R.
Proceedings of the First West Coast Computer Faire, April, 1977

MCALL-C: A Communications Protocol for Personal Computers
Pugh
Dr. Dobbs Journal, 1980, No. 46, P. 16.

Satellite-Linked Computer Network, A Phase-III Hook-up for Your Keyboard
Riportella, Vern, WA2LQQ, AMICON Coordinator, Box 56, Warwick, NY 10990
HAM Radio Horizons, March, 1980, pp. 48-51.

The Packet Radio Revolution
Rouleau, Bob
73 Magazine, December 1978, p. 192.

Packet Radio
Rouleau and Hodgson
Tab Books, Blue Ridge Summit, PA, 1981

Personal Computers in a Distributed Communications Network
Steinwedel, Jeff, W3FY, 715 Reseda Drive, Apt.2, Sunnyvale, CA 94087
BYTE, Vol. 3 No. 2, p. 80, February, 1978

Calling All Computers
Stoner, Donald L., W6TNS/7, John Hancock Bldg., Mercer Island, WA 98040
BYTE, Vol. 3 No. 12, p. 159, December, 1978

Computer Networks
Tesler, L.
People's Computers, Vol. 6. No. 2, Sep-Oct 1977

A Network of Community Information Exchanges: Issues And Problems
Wilber, M
Proceedings of the First West Coast Computer Faire, April, 1977

CIE Net: A Design for a Network of Community Information Exchanges -- Part 1
Wilber, Mike, 920 Dennis Drive, Palo Alto, CA 94303
BYTE, Vol. 3 No. 2, p. 14, February, 1978

CIE Net: Protocols -- Part 2
Wilber, Mike, 920 Dennis Drive, Palo Alto, CA 94303
BYTE, Vol. 3 No. 3, p. 152, March, 1978

CIE Net: Other Considerations -- Part 3
Wilber, Mike, 920 Dennis Drive, Palo Alto, CA 94303
BYTE, Vol. 3 No. 4, p. 168, April, 1978

ASCII at Last?
Williams, Perry F., W1UED
QST, Vol. LXII No. 10, p. 54, October, 1978

REFERENCES ON SATELLITE PACKET COMMUNICATIONS

The ALOHA System
Abramson, Norman
Computer Communications Networks, Prentice Hall, Inc., 1973, pp. 501-518.

The Throughput of Packet Broadcasting Channels
Abramson, Norman
IEEE Trans. on Communications, Vol. COM-25, No. 1, January, 1977, pp. 117-128.
Reprinted in "Satellite Communications", Harry L. Van Trees, Ed., IEEE Press

Closed Loop Stability Controls for S-ALOHA Satellite Communication
Gerla, M. and Kleinrock, L.
Proc. Fifth Data Communications Symposium, Snowbird, Utah, September, 1977.

Special Issue on Computer Network Architectures and Protocols
Green, P. E., Editor
IEEE Trans. on Communications, Vol. COM-28, No. 4, April, 1980

Advances in Packet Radio Technology
Kahn, et al.
Proceedings of the IEEE, Vol. 66, No. 11, November 1978

Packet Switching in Radio Channels: Part I - Carrier Sense Multiple Access Modes and their Throughput Delay Characteristics
Klienrock, L. and Tobagi
IEEE Transactions On Communications, Vol. COMM-23, December 1975, pp 1400-1416.

Satellite Packet Communication - Multiple Access Protocols and Performance
Lam, Simon S.
IEEE Trans. on Communications, Vol. COM-27, No. 10, October, 1979, pp. 1456-1466

Appendix B - ISO Specification 3309 - 1976 (E)

Data communication — High-level data link control procedures — Frame structure

0 INTRODUCTION

This document is one of a series of International Standards, to be used for implementation of various applications with synchronous transmission facilities.

1 SCOPE AND FIELD OF APPLICATION

This International Standard defines in detail the frame structure for data communication systems using bit-oriented high-level data link control (HDLC) procedures. It defines the relative positions of the various components of the basic frame and the bit combination for the frame delimiting sequence (Flag). The bit escaping mechanism which is used to achieve bit pattern independence within the frame is also defined. The document also specifies the frame checking sequence (FCS). No details of the address or control field allocations are included, other than address extension outlined in clause 4.

2 FRAME STRUCTURE

In HDLC, all transmissions are in frames, and each frame conforms to the following format :

Flag	Address	Control	Information	FCS	Flag
01111110	8 bits	8 bits	*	16 bits	01111110

* An unspecified number of bits which in some cases may be a multiple of a particular character size, for example an octet.

where

Flag = flag sequence

Address = secondary station address field

Control = control field

Information = information field

FCS = frame checking sequence

Frames containing only supervisory control sequences form a special case where there is no information field. The format for these frames shall be :

Flag	Address	Control	FCS	Flag
01111110	8 bits	8 bits	16 bits	01111110

3 ELEMENTS OF THE FRAME

3.1 Flag sequence

All frames shall start and end with the flag sequence. All stations which are attached to the data link shall continuously hunt for this sequence. Thus, the flag is used for frame synchronization. A single flag may be used as both the closing flag for one frame and the opening flag for the next frame.

3.2 Address field

The address shall in all cases identify the secondary or secondaries which are involved in the particular frame interchange.

3.3 Control field

The control field contains commands or responses, and sequence numbers. The control field shall be used by the primary to command the addressed secondary to perform a particular operation. It shall be used by the secondary to respond to the primary.

3.4 Information field

Information may be any sequence of bits. In most cases it will be linked to a convenient character structure, for example octets, but if required, it may be an unspecified number of bits and unrelated to a character structure.

3.5 Transparency

The transmitter shall examine the frame content between the two flag sequences including the address, control and FCS sequences and shall insert a "0" bit after all sequences of 5 contiguous "1" bits (including the last 5 bits of the FCS) to ensure that a flag sequence is not simulated. The receiver shall examine the frame content and shall discard any "0" bit which directly follows 5 contiguous "1" bits.

3.6 Frame checking sequence (FCS)

The FCS shall be a 16-bit sequence. It shall be the ones complement of the sum (modulo 2) of :

1) the remainder of x^k $(x^{15} + x^{14} + x^{13} + \ldots + x^2 + x + 1)$ divided (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$, where k is the number of bits in the frame existing between, but not including, the final bit of the opening flag and the first bit of the FCS, excluding bits inserted for transparency, and

2) the remainder after multiplication by x^{16} and then division (modulo 2) by the generator polynomial $x^{16} + x^{12} + x^5 + 1$ of the content of the frame, existing between, but not including, the final bit of the opening flag and the first bit of the FCS, excluding bits inserted for transparency.

As a typical implementation, at the transmitter, the initial remainder of the division is preset to all ones and is then modified by division by the generator polynomial (as described above) on the Address, Control and Information fields; the ones complement of the resulting remainder is transmitted as the 16-bit FCS sequence.

At the receiver, the initial remainder is preset to all ones and the serial incoming protected bits and the FCS when divided by the generator polynomial will result in a remainder of 0001110100001111 (x^{15} through x^0, respectively) in the absence of transmission errors.

NOTES

1 If future applications show that a higher degree of protection is needed, the number of bits of the FCS shall be increased by octets.

2 See the annex for explanatory notes on implementation of the FCS.

3.7 Order of bit transmission

Addresses, commands, responses, and sequence numbers shall be transmitted low-order bit first (for example the first bit of the sequence number that is transmitted shall have the weight 2^0).

The order of transmitting bits within the information field is not specified by this International Standard.

The FCS shall be transmitted to the line commencing with the coefficient of the highest term.

3.8 Inter-frame time fill

Inter-frame time fill shall be accomplished by transmitting either contiguous flags or a minimum of seven contiguous "1" bits or a combination of both.

A selection of the inter-frame time fill methods depends on systems requirement.

3.9 Invalid frame

An invalid frame is defined as one that is not properly bounded by two flags or one which is too short (for example shorter than 32 bits between flags). Invalid frames shall be ignored. Thus, a frame which ends with an all "1" bit sequence equal to or greater than seven bits in duration shall be ignored.

As an example, one method of aborting a frame would be to transmit 8 contiguous "1" bits.

4 EXTENSIONS

4.1 Extended address field

Normally a single octet address shall be used and all 256 combinations shall be available.

However, by prior agreement the address range can be extended by reserving the first transmitted bit (low order) of each address octet which would then be set to binary zero to indicate that the following octet is an extension of the basic address. The format of the extended octet(s) shall be the same as that of the basic octet. Thus, the address field may be recursively extended.

When extensions are used, the presence of a binary "1" in the first transmitted bit of the basic address octet signals that only one address octet is being used. The use of address extension thus restricts the range of single octet addresses to 128.

4.2 Extended control field

The control field may be extended by one or more octets. The extension method and the bit patterns for the commands and responses will be defined in a separate International Standard.

ANNEX

EXPLANATORY NOTES ON IMPLEMENTATION OF THE FRAME CHECKING SEQUENCE

(Not part of the standard)

In order to permit the use of existing devices that are arranged to use a zero preset register, the following implementation may be used.

At the transmitter, generate the FCS sequence in the following manner while transmitting the elements of the frame unaltered onto the line :

a) preset the FCS register to zeros;

b) invert the first 16 bits (following the opening flag) before shifting into the FCS register;

c) shift the remaining fields of the frame into the FCS register uninverted;

d) invert the contents of the FCS register (remainder) and shift onto the line as the FCS sequence.

At the receiver, operate the FCS checking register in the following manner while receiving (and storing) unaltered the elements of the frame as received from the line :

a) preset the FCS register to zeros;

b) invert the first 16 bits (following the opening flag) before shifting them into the FCS checking register;

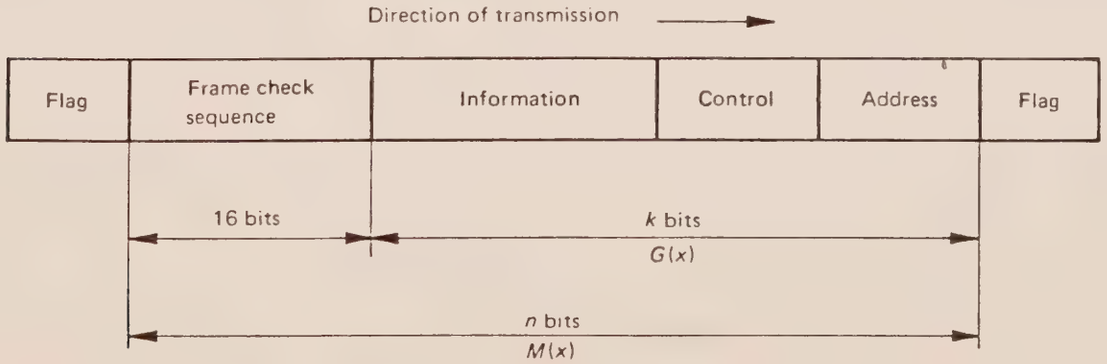
c) shift the remaining elements of the frame, up to the beginning of the FCS, into the checking register uninverted;

d) invert the FCS sequence before shifting into the checking register. In the absence of errors, the FCS register will contain all zeros after the FCS is shifted in.

In the above, inversion of the first 16 bits is equivalent to a ones preset and inversion of the FCS at the receiver causes the registers to go to the all zeros state.

The transmitter or the receiver can independently use the ones preset or the first 16-bit inversion. Also, the receiver can choose not to invert the FCS, in which case it must check for the unique non-zero remainder specified in 3.6.

It must be realized that inversion of the FCS by the receiver requires a 16-bit storage delay before shifting message bits into the register. The receiver cannot anticipate the beginning of the FCS. Such storage, however, will normally take place naturally as the FCS checking function will need to differentiate the FCS from data anyway, and it will thus withhold 16 bits from the next function at all times.



The procedure for using the FCS assumes the following :

1) The k bits of data which are being checked by the FCS can be represented by a polynomial $G(x)$.

Example : $G(x) = x^5 + x^3 + 1$ represents 101001.

2) The Address field, Control field and Information field (if it exists in the message) are represented by the polynomial $G(x)$.

3) For the purpose of generating the FCS, the first bit following the opening flag is the most significant bit of $G(x)$ regardless of the actual representation of the Address, Control and Information fields.

4) There exists a generator polynomial $P(x)$ of degree 16, having the form $P(x) = x^{16} + x^{12} + x^5 + 1$.

The FCS is defined as a ones complement of a remainder, $R(x)$, obtained from the modulo 2 division of

$$x^{16}G(x) + x^k\,(x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x^1 + 1)$$

by the generator polynomial $P(x)$.

$$\frac{x^{16}G(x) + x^k\,(x^{15} + x^{14} + \ldots + x + 1)}{P(x)} = Q(x) + \frac{R(x)}{P(x)} \longleftarrow \overline{\text{FCS}}$$

The multiplication of $G(x)$ by x^{16} corresponds to shifting the message $G(x)$ 16 places and thus providing the space of 16 bits for the FCS.

The addition of $x^k\,(x^{15} + x^{14} + \ldots + x + 1)$ to $x^{16}G(x)$ (equivalent to inverting the first 16 bits of $x^{16}G(x)$) corresponds to initializing the initial remainder to a value of all "ones". This addition is provided for the purpose of protection against the obliteration of leading flags, which may be non-detectable if the initial remainder is zero. The complementing of $R(x)$, by the transmitter, at the completion of the division ensures that the received, error-free message will result in a unique, non-zero remainder at the receiver. The non-zero remainder provides protection against potential non-detectability of the obliteration of trailing flags.

At the transmitter the FCS is added to the $x^{16}G(x)$ and results in the total message $M(x)$ of length n, where $M(x) = x^{16}G(x) + \text{FCS}$.

At the receiver, the incoming $M(x)$ is multiplied by x^{16}, added to $x^n\,(x^{15} + x^{14} + \ldots + x + 1)$ and divided by $P(x)$.

$$\frac{x^{16}\,[x^{16}G(x) + \text{FCS}] + x^n\,(x^{15} + x^{14} + \ldots + x + 1)}{P(x)} = Qr(x) + \frac{Rr(x)}{P(x)}$$

If the transmission is error free, the remainder $Rr(x)$ will be "ϕϕϕ111ϕ1ϕϕϕϕ1111" (x^{15} through x^0).

$Rr(x)$ is the remainder of the division : $\dfrac{x^{16}L(x)}{P(x)}$

where $L(x) = x^{15} + x^{14} + \ldots + x + 1$. This can be shown by establishing that all other terms of the numerator of the receiver division are divisible by $P(x)$.

Note that $\text{FCS} = \overline{R(x)} = L(x) + R(x)$. (Adding $L(x)$ without carry to a polynomial of its same length is equivalent to a bit-by-bit inversion of the polynomial.)

The equation above, for the FCS receiver residual, is used in the following to show that inverting the FCS at the receiver returns the checking register to zero. This equation is

$$\frac{x^{16}L(x)}{P(x)} = Q(x) + \frac{Rr(x)}{P(x)}$$

where $L(x)$ is as before and $Rr(x)$ is the residual contents of the FCS register.

If another $x^{16}L(x)$ is added to the above numerator, the result is

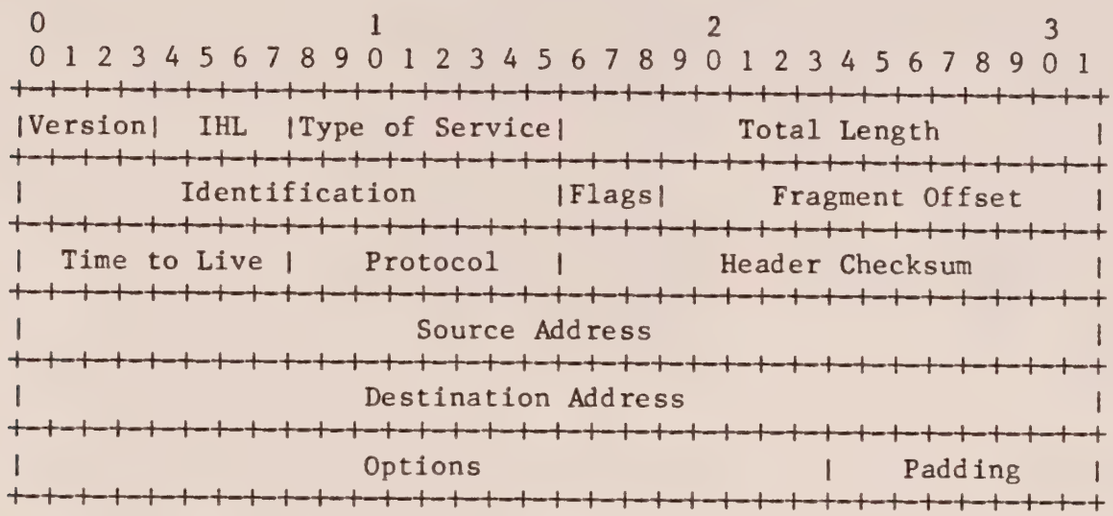
$$\frac{x^{16}L(x) + x^{16}L(x)}{P(x)} = 0$$

Physically, this second $x^{16}L(x)$ quantity is added to the bit stream by inverting the FCS.

Appendix C - INTERNET Protocol Specification, January 1980 Revision

Internet Header Format

A summary of the contents of the internet header follows:



Example Internet Datagram Header

Figure 3.

Note that each tick mark represents one bit position.

Version: 4 bits

The Version field indicates the format of the internet header. This document describes version 4.

IHL: 4 bits

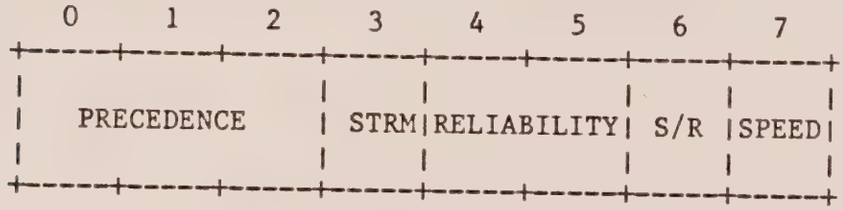
Internet Header Length is the length of the internet header in 32 bit words, and thus points to the beginning of the data. Note that the minimum value for a correct header is 5.

Type of Service: 8 bits

The Type of Service provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Several networks offer service precedence, which somehow treats high precedence traffic as more important than other traffic. A few networks offer a Stream service, whereby one can achieve a smoother service at some cost. Typically this involves the reservation of resources within the network. Another choice involves a low-delay vs. high-reliability trade off. Typically networks invoke more

complex (and delay producing) mechanisms as the need for reliability increases.

Bits 0-2: Precedence.
Bit 3: Stream or Datagram.
Bits 4-5: Reliability.
Bit 6: Speed over Reliability.
Bits 7: Speed.



PRECEDENCE	STRM	RELIABILITY	S/R	SPEED
111-Flash Override	1-STREAM	11-highest	1-speed	1-high
110-Flash	0-DTGRM	10-higher	0-rlblt	0-low
11X-Immediate		01-lower		
01X-Priority		00-lowest		
00X-Routine				

The type of service is used to specify the treatment of the datagram during its transmission through the internet system. In the discussion (section 3.2) below, a chart shows the relationship of the internet type of service to the actual service provided on the ARPANET, the SATNET, and the PRNET.

Total Length: 16 bits

Total Length is the length of the datagram, measured in octets, including internet header and data. This field allows the length of a datagram to be up to 65,535 octets. Such long datagrams are impractical for most hosts and networks. All hosts must be prepared to accept datagrams of up to 576 octets (whether they arrive whole or in fragments). It is recommended that hosts only send datagrams larger than 576 octets if they have assurance that the destination is prepared to accept the larger datagrams.

The number 576 is selected to allow a reasonable sized data block to be transmitted in addition to the required header information. For example, this size allows a data block of 512 octets plus 64 header octets to fit in a datagram. The maximal internet header is 60 octets, and a typical internet header is 20 octets, allowing a margin for headers of higher level protocols.

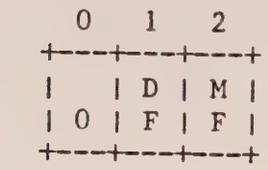
Identification: 16 bits

An identifying value assigned by the sender to aid in assembling the fragments of a datagram.

Flags: 3 bits

Various Control Flags.

Bit 0: reserved, must be zero
Bit 1: Don't Fragment This Datagram (DF).
Bit 2: More Fragments Flag (MF).



Fragment Offset: 13 bits

This field indicates where in the datagram this fragment belongs. The fragment offset is measured in units of 8 octets (64 bits). The first fragment has offset zero.

Time to Live: 8 bits

This field indicates the maximum time the datagram is allowed to remain the internet system. If this field contains the value zero, then the datagram should be destroyed. This field is modified in internet header processing. The time is measured in units of seconds. The intention is to cause undeliverable datagrams to be discarded.

Protocol: 8 bits

This field indicates the next level protocol used in the data portion of the internet datagram. The values for various protocols are specified in reference [6].

Header Checksum: 16 bits

A checksum on the header only. Since some header fields may change (e.g., time to live), this is recomputed and verified at each point that the internet header is processed.

The checksum algorithm is:

The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.

This is a simple to compute checksum and experimental evidence indicates it is adequate, but it is provisional and may be replaced by a CRC procedure, depending on further experience.

Source Address: 32 bits

The source address. The first octet is the Source Network, and the following three octets are the Source Local Address.

Destination Address: 32 bits

The destination address. The first octet is the Destination Network, and the following three octets are the Destination Local Address.

Options: variable

The option field is variable in length. There may be zero or more options. There are two cases for the format of an option:

Case 1: A single octet of option-type.

Case 2: An option-type octet, an option-length octet, and the actual option-data octets.

The option-length octet counts the option-type octet and the option-length octet as well as the option-data octets.

The option-type octet is viewed as having 3 fields:

1 bit reserved, must be zero
2 bits option class,
5 bits option number.

The option classes are:

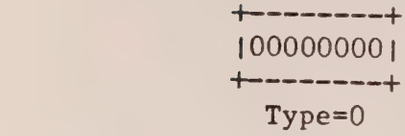
0 = control
1 = internet error
2 = experimental debugging and measurement
3 = reserved for future use

The following internet options are defined:

CLASS	NUMBER	LENGTH	DESCRIPTION
0	0	-	End of Option list. This option occupies only 1 octet; it has no length octet.
0	1	-	No Operation. This option occupies only 1 octet; it has no length octet.
0	2	4	Security. Used to carry Security, and user group (TCC) information compatible with DOD requirements.
0	3	var.	Source Routing. Used to route the internet datagram based on information supplied by the source.
0	7	var.	Return Route. Used to record the route an internet datagram takes.
0	8	4	Stream ID. Used to carry the stream identifier.
1	1	var.	General Error Report. Used to report errors in internet datagram processing.
2	4	6	Internet Timestamp.
2	5	6	Satellite Timestamp.

Specific Option Definitions

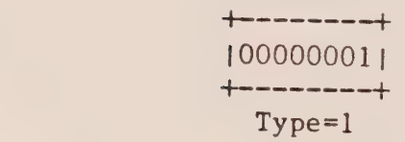
End of Option List



This option indicates the end of the option list. This might not coincide with the end of the internet header according to the internet header length. This is used at the end of all options, not the end of each option, and need only be used if the end of the options would not otherwise coincide with the end of the internet header.

May be copied, introduced, or deleted on fragmentation.

No Operation

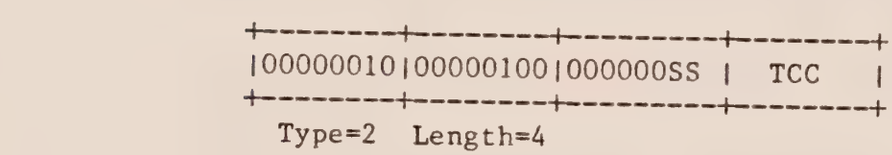


This option may be used between options, for example, to align the beginning of a subsequent option on a 32 bit boundary.

May be copied, introduced, or deleted on fragmentation.

Security

This option provides a way for DOD hosts to send security and TCC (closed user groups) parameters through networks whose transport leader does not contain fields for this information. The format for this option is as follows:



Security: 2 bits

Specifies one of 4 levels of security

11-top secret
10-secret
01-confidential
00-unclassified

Transmission Control Code: 8 bits

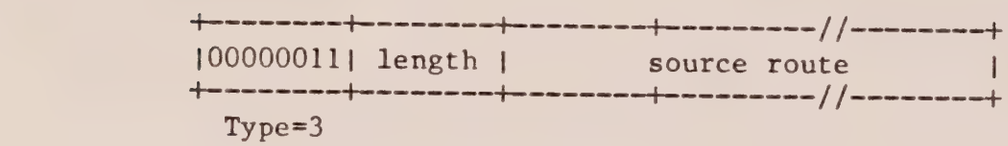
Provides a means to compartmentalize traffic and define controlled communities of interest among subscribers.

Note that this option does not require processing by the

internet module but does require that this information be passed to higher level protocol modules. The security and TCC information might be used to supply class level and compartment information for transmitting datagrams into or through AUTODIN II.

Must be copied on fragmentation.

Source Route



The source route option provides a means for the source of an internet datagram to supply routing information to be used by the gateways in forwarding the datagram to the destination.

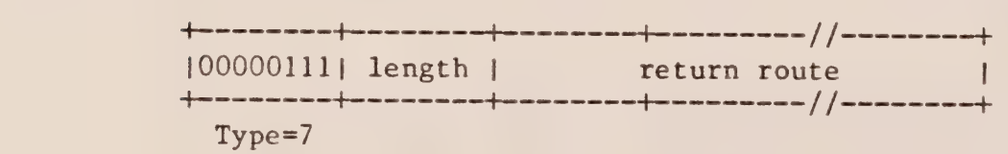
The option begins with the option type code. The second octet is the option length which includes the option type code and the length octet, as well as length-2 octets of source route data.

A source route is composed of a series of internet addresses. Each internet address is 32 bits or 4 octets. The length defaults to two, which indicates the source route is empty and the remaining routing is to be based on the destination address field.

If the address in destination address field has been reached and this option's length is not two, the next address in the source route replaces the address in the destination address field, and is deleted from the source route and this option's length is reduced by four. (The Internet Header Length Field must be changed also.)

Must be copied on fragmentation.

Return Route



The return route option provides a means to record the route of an internet datagram.

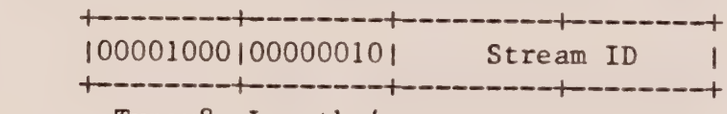
The option begins with the option type code. The second octet is the option length which includes the option type code and the length octet, as well as length-2 octets of return route data.

A return route is composed of a series of internet addresses. The length defaults to two, which indicates the return route is empty.

When an internet module routes a datagram it checks to see if the return route option is present. If it is, it inserts its own internet address as known in the environment into which this datagram is being forwarded into the return route at the front of the address string and increments the length by four.

Not copied on fragmentation, goes in first fragment only.

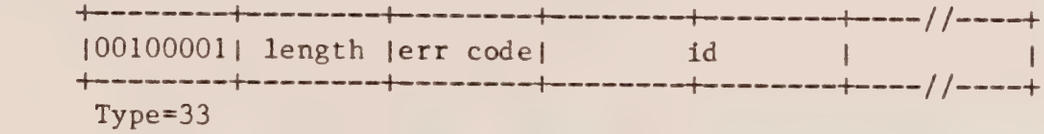
Stream Identifier



This option provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.

Must be copied on fragmentation.

General Error Report



The general error report is used to report an error detected in processing an internet datagram to the source internet module of that datagram. The "err code" indicates the type of error detected, and the "id" is copied from the identification field of the datagram in error, additional octets of error information may be present depending on the err code.

If an internet datagram containing the general error report option is found to be in error or must be discarded, no error report is sent.

ERR CODE:

0 - Undetermined Error, used when no information is available about the type of error or the error does not fit any defined class. Following the id should be as much of the datagram (starting with the internet header) as fits in the option space.

1 - Datagram Discarded, used when specific information is available about the reason for discarding the datagram can be reported. Following the id should be the original (4-octets) destination address, and the (1-octet) reason.

Reason	Description

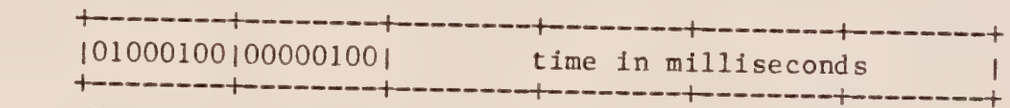
0 No Reason
1 No One Wants It - No higher level protocol or application program at destination wants this datagram.
2 Fragmentation Needed & DF - Cannot deliver with out fragmenting and has don't fragment bit set.
3 Reassembly Problem - Destination could not reassemble due to missing fragments when time to live expired.
4 Gateway Congestion - Gateway discarded datagram due to congestion.

The error report is placed in a datagram with the following values in the internet header fields:

Version: Same as the datagram in error.
IHL: As computed.
Type of Service: Zero.
Total Length: As computed.
Identification: A new identification is selected.
Flags: Zero.
Fragment Offset: Zero.
Time to Live: Sixty.
Protocol: Same as the datagram in error.
Header Checksum: As computed.
Source Address: Address of the error reporting module.
Destination Address: Source address of the datagram in error.
Options: The General Error Report Option.
Padding: As needed.

Not copied on fragmentation, goes with first fragment.

Internet Timestamp

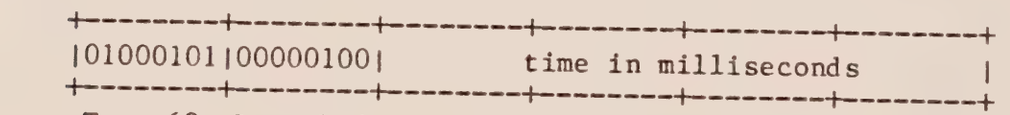


Type=68 Length=6

The data of the timestamp is a 32 bit time measured in milliseconds.

Not copied on fragmentation, goes with first fragment

Satellite Timestamp



Type=69 Length=6

The data of the timestamp is a 32 bit time measured in milliseconds.

Not copied on fragmentation, goes with first fragment

Padding: variable

The internet header padding is used to ensure that the internet header ends on a 32 bit boundary. The padding is zero.

Appendix D - Distribution List

Dave Altekruse, W6RAW
1614 164th Avenue, San Leandro, CA 94578
Home: 415-276-4130 Office: 414-367-3137

David W. Borden, K8MMO
Route 2, Box 233B, Sterling, VA 22170
Home: 703-430-7642 Office:

Bob Bruninga, WB4APR, Director and Computer Trustee of AMRAD
907 Ninovan Road, Vienna, VA 22180
Home: Office:

Bob Carpenter, W3OTC
12708 Circle Drive, Rockville, MD 20850
Home: Office:

Dr. Tom Clark, W3IWI, AMSAT Director & Executive Vice President
6388 Guilford Rd., Clarksville, MD 21029
Home: 301-286-3113 Office: 301-344-5957

Mark Corbitt, WB4FNE/6, Data Communications Advisor to the ARRL
6568 Beachview Drive, No. 311, Rancho Palos Verdes, CA 90274
Home: 213-377-1385 Office: 213-535-4321

Dr. John DuBois, W1HDX, AMSAT Special Systems Consultant
241 Crescent Ave., Waltham, MA 02154
Home: 617-263-7004 Office: 617-891-9029

David C. Engle
1063 Summerwood Court, San Jose, CA 95132
Home: 408-251-2910 Office: 415-494-7400 x5630

J. E. Fail
6170 Downey Avenue, Long Beach, CA 908055070
Home: 213-531-4852 Office:

Gary Fariss, W6KYF
18983 Saratoga Glen Place, Saratoga, CA 95070
Home: 408-257-0948 Office: 408-734-6857

John Gilmore
401-1/2 Clayton Street, San Francisco, CA 94117
Home: 415-864-2891 Office: 415-864-2891

Joe Kasser, G3ZCZ, Editor of ORBIT Magazine
AMSAT, P. O. Box 27, Washington, D.C. 20044
Home: Office: 301-840-5600 x308

Mark Kaufmann, WB6ECE
14100 Donelson Place, Los Altos Hills, CA 94022
Home: 415-948-3777 Office: 415-962-8811

Larry Kayser, VE3QB
24 Arundel Ave., Ottawa, Ontario Canada K1K 0B6
Home: Office:

R. Alan Larson
SRI International, 333 Ravenswood Avenue, Menlo Park, CA 94025
Home: Office: 415-859-5640

Wally Linstruth, WA6JPR
2413 Burritt Ave., Redondo Beach CA 90378
Home: 213-542-3290 Office:

Robert C. Livingston, VE7CYB
#904 - 1075 Comox Street, Vancouver, B.C., Canada V6E 1K2
Home: 604-689-9563 Office:

Doug Lockhart, VE7APU
Vancouver Dig. Comm. Group, 1263 Balfour Ave., Vancouver, B. C. Canada V6H 1X6
Home: 604-738-5683 Office:

Dr. H. S. Magnuski, KA6M, AMICON Network Consultant
311 Stanford Ave., Menlo Park, CA 94025
Home: 415-854-1927 Office: 415-856-7421

Dr. John Pronko, W6XO, President, Project OSCAR
230 Hawthorne Ave., Los Altos, CA 94022
Home: 415-941-6988 Office: 415-493-4411 x45179

William Putney, WB6RFW
Tymnet, Inc., 10161 Bubb Road, Cupertino, CA 95014
Home: 408-446-7190 Office: 408-446-7190

Vern Riportella, WA2LQQ, AMICON Coordinator
Box 56, Warwick, NY 10990
Home: 914-986-6904 Office: 201-768-2500

Bob Rouleau, VE2PY
1050 Churchill, Mt. Royal, Quebec H3R 3B6
Home: 514-341-7806 Office:

R. Satterlee, WB6VAL
1212 W. McKinley, Apt. 5, Sunnyvale, CA 94086
Home: 415-969-4451 Office: 415-964-5700 x227

Calvin Teague, K6HWJ
2046 Kent Drive, Los Altos, CA 94022
Home: 415-967-2807 Office: 415-497-3596

Rich Zwirko, K1HTV, AMSAT Director and Vice President
34 Montclair Dr., Manchester, CT 06040
Home: 203-646-5726 Office: 203-522-1080

Appendix E - Document Revision History

DOCUMENT REVISION HISTORY

1.00	March, 1980	Outline of specification
1.01	April, 1980	Initial draft with first set of proposals
1.02	October, 1981	Major revision incorporating INTERNET spec